UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/758,434	01/14/2004	Feisal Y. Daruwalla	CISCP134C1/8803	5662

22434 7590 06/26/2007

BEYER WEAVER LLP
P.O. BOX 70250
OAKLAND, CA 94612-0250

EXAMINER	
SAMUEL, DEWANDA A	
ART UNIT	**PAPER NUMBER**
2616	

MAIL DATE	DELIVERY MODE
06/26/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

SF

Office Action Summary	Application No.	Applicant(s)	
	10/758,434	DARUWALLA ET AL.	
	Examiner	Art Unit	
	DeWanda Samuel	2616	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 January 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-11* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-11* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *10 December 2004*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. **Claim 7** objected to because of the following informalities: "The apparatus of claim 22". Appropriate correction is required.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

4. **Claims 1, 2, and 7** are rejected under 35 U.S.C. 103(a) as being unpatentable over Fijolek et al. (US Patent 6,510,162) in view of Gilbrech (US Patent 6,173,399).

With regard to claim 1, Fijolek et al. discloses having an *apparatus for routing packets from a first network node to a second network node in a data network,* Fijolek et al. discloses having a cable modem termination system 12 in fig .1 in a cable network

that is routing data from a from a cable modem ("first network node" back to a cable modem ("second network node ", fig. 5).

comprising: means for assigning an ID to the first node that is associated with at least on VPN, wherein the ID is assigned by an entity other than the first node; Fijolek et al. discloses having a cable modem termination system 12 in fig. 1 that assigns service identifiers (SIDs) to CM (cable modems, column 15 line 17-18). However, Fijolek et al. does not disclose first node associated with at least on VPN, wherein the ID is assigned by an entity other than the first node. Gilbrech discloses having a apparatus for implementing a Virtual Private Networks (title). Gilbrech further discloses the VPN unit moderates data communication between members of a defined VPN group (column 2 line 45-48)...the VPN unit maintains a lookup table identifying members of a specific virtual private network groups. It is inferred that the VPN unit keeps record of an identifier of member in a table and each identifier is link to a virtual private network groups.

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to have a to a cable modem termination system 12 (CMTS) as taught by Fijolek et al. with a VPN unit that associates identifying members with a virtual private network groups as taught by Gilbrech to provide a more secure cable network.

means for receiving a packet from the first node, said packet including the ID associated with said first node, and including routing information for routing said packet to a

destination address associated with said second node; Fijolek et al. discloses having a packet format for a incoming packet being received form a CM (cable modem, column 15 table 9 and 10 line 25-67).

means for examining the packet to identify the ID of the first node; Fijolek et al. discloses the cable modem termination system 12 (CMTS) have the means of examining incoming packets with service identifiers (SID, column 15 line10-67).

and means for using said first node ID and routing information to determine whether said first node is associated with at least one VPN. Fijolek et al. discloses having a unique service identifier (SID) corresponding to a cable modem (CM) and the SID and routing information transmitted in a packet. However, Fijolek et al. does not disclose first node is associated with at least one VPN. Gilbrech discloses having a VPN unit processing packet by examining the source and destination address of the packet. Gibrech further discloses the VPN unit moderates data communication between members of a defined VPN group (column 2 line 45-48)...the VPN unit maintains a lookup table identifying members of a specific virtual private network groups. It is inferred that the VPN unit keeps record of an identifier of member in a table and each identifier is link to a virtual private network groups.

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to have a to a cable modem termination system 12 (CMTS) assigning a unique identifier SID within a packet as taught by Fijolek et al.

being examined a VPN unit that associates identifying members with a virtual private network groups as taught by Gilbrech to provide a more secure cable network.

With regard to claim 2, in combination Fijolek et al. and Gibrech teaches the apparatus recited in claim 1.*Further comprising means for routing the packet to the second node.* Fijolek et al. discloses in fig. 1 that the cable modem termination system 12 (CMTS) has the means to transmit a packet to a second CM (cable modem).

With regard to claim 7, in combination Fijoleck and Gibrech teaches the apparatus recited in claim 2. *further comprising: means for receiving at said Head End device a packet from said first node, said packet including a destination address corresponding to a second node in the network;* Fijolek et al. discloses having a head end of a cable system 26 in fig.1which has the means to send and receive packets from cable modems...such configurations may be "one-to-one", "one-to-many" or "many –to-many" (column 7 line 20-38). Fijolek et al. further discloses having

means for examining said packet to identify the ID of said first node; Fijolek et al. discloses the cable modem termination system 12 (CMTS) have the means of examining incoming packets with service identifiers (SID, column 15 line10-67).

and means for using said ID at said Head End device to determine whether said first node is a member of at least one VPN. Fijoleck et al. discloses having a cable modem

termination system 12a-c...also Fijoleck et al discloses a cable television network headend is a central location (column 4 line 33-34). However, Fijoleck et al. does not disclose first node is a member of at least one VPN. . Gilbrech discloses having a VPN unit processing packet by examining the source and destination address of the packet. Gibrech further discloses the VPN unit moderates data communication between members of a defined VPN group (column 2 line 45-48)...the VPN unit maintains a lookup table identifying members of a specific virtual private network groups. It is inferred that the VPN unit keeps record of an identifier of member in a table and each identifier is link to a virtual private network groups.

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to have a to a cable modem termination system 12 (CMTS) assigning a unique identifier SID within a packet as taught by Fijolek et al. being examined a VPN unit that associates identifying members with a virtual private network groups as taught by Gilbrech to provide a more secure cable network

5. **Claims 3-6 and 8-9** are rejected under 35 U.S.C. 103(a) as being unpatentable over Fijolek et al. (US Patent 6,577,642) in view of Rosen et al. ("BGP/MPLS VPNs" 1999).

With regard to claim 3, Fijolek et al. discloses having *an apparatus of associating nodes in a data network with at least one virtual private network (VPN), the data network including an access network having at least one Head End device and a*

plurality of nodes, the access network further including at least one shared access channel utilized by a first and a second node of the plurality of nodes to communicate with the Head End device, Fijolek et al. discloses having a cable modem termination system 12 in fig 1 located in a head end of cable system 26 (fig.1). It is conventional that a cable modem termination system can operate as point-to-point or point-to-multipoint and that the cable modem are bi-directionally communicating with the head end. Fijolek et al. discloses having a virtual networking administration in a data-over-cable-system 10 using a network address and the first virtual networking tag stored in a virtual networking table associated with the second network device to provide selected first network devices a desired networking service on a virtual network via the data-over-cable-system (column 28 line 34-43).

said apparatus comprising: means for assigning an address to the first node that is associated with at least one VPN, wherein the address is assigned by an entity other than the first node; Fijolek et al. discloses having a dynamic network host configuration server 66 used to allocate network host address (e.g. head end) and deliver configuration parameters to dynamically configured network host clients (column 13 line 45-58). Fijolek further discloses that network address such as IP addresses are assigned to network devices such as the CM (cable modem) 16 are typically assigned by a data-over-cable-system 10 using DHCP 66 (column 28 line 1-4).
means for receiving a communication from the first node in the access network; Fijolek et al. discloses that the CMTS receives communication via DHCP 66 layer from the CM

16 (cable modem, column 13 line 5-22). Fijolek et al. discloses having a virtual networking administration in a data-over-cable-system 10 using a network address and the first virtual networking tag stored in a virtual networking table associated with the second network device to provide selected first network devices a desired networking service on a virtual network via the data-over-cable-system (column 28 line 34-43).

means for identifying the address of the first node, wherein the address is specific to the network on which the first node resides; Fijolek et al. discloses identifying the CM 16 network address (column 21 line 3-30).

Fijolek et al. does not disclose having the means for using said address to determine whether said first node is associated with at least one VPN. *Rosen et al. discloses having a method in which a service provider with a IP backbone may provide VPNs (Virtual Private Networks) for its customers with MPLS (Multiprotocol Label Switching) is used for forwarding packets over the backbone (Abstract).* Rosen et al. further discloses having a labeled packets ("assigned ID") being associated with specific VPNs (page 16 line paragraph 8.1 line 1-12). It is inferred that the labels indicate which VPN the packet via device or node is destined for.

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to have a virtual networking administration in a data-over-cable-system 10 as taught by Fijolek et al. (6,577,642) with a mechanism that will label packet with corresponding VPNs as taught by Rosen et al. to provide a

mechanism that will transmit packets via device or node to there appropriate VPN.

With regard to claim 4, in combination Fijolek et al. and Rosen et al. teaches the apparatus in claim 3. *further comprising means for mapping said first node to a particular sub-interface on the access network.* Fijolek et al. discloses having a virtual networking administration in a data-over-cable-system 10 using a network address and the first virtual networking tag stored in a virtual networking table associated with the second network device to provide selected first network devices a desired networking service on a virtual network via the data-over-cable-system (column 28 line 34-43). However, Fijolek et al. does not disclose means for mapping said first node to a particular sub-interface on the access network. Rosen et al. discloses that one could divide the interface into multiple "sub-interfaces"... and assign the packets to a VPN based on the on the sub-interface over which it arrives (page 7 paragraph 3.1 line 11-17).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to have a virtual networking administration in a data-over-cable-system 10 as taught by Fijolek et al. assign the packets to a VPN based on the on the sub-interface over which it arrives as taught by Rosen et al. to provide a mechanism that will prevent packets from entering in a VPN that is not associated with it.

With regard to claim 5, Fijolek et al. discloses a*n apparatus of associating nodes in a data network with at least one virtual private network (VPN), the data*

network including an access network having at least one Head End device and a plurality of nodes, the access network further including at least one shared access channel utilized by a first and a second node of the plurality of nodes to communicate with the Head End device, Fijolek et al. discloses having a cable modem termination system 12 in fig 1 located in a head end of cable system 26 (fig.1). It is conventional that a cable modem termination system can operate as point-to-point or point-to-multipoint and that the cable modem are bi-directionally communicating with the head end. Fijolek et al. discloses having a virtual networking administration in a data-over-cable-system 10 using a network address and the first virtual networking tag stored in a virtual networking table associated with the second network device to provide selected first network devices a desired networking service on a virtual network via the data-over-cable-system (column 28 line 34-43).

Fijolek et al. does not discloses *said apparatus comprising: means for determining whether said first node is a member of at least one VPN;* Rosen et al. discloses having a method in which a service provider with an IP backbone may provide VPNs (Virtual Private Networks) for its customers with MPLS (Multiprotocol Label Switching) is used for forwarding packets over the backbone (Abstract). It is inferred that this mechanism can be implemented in the head end of a cable system 26. Rosen et al. further discloses assigning packets to a particular site (page 7 line 12-13)...also a packet's destination address is matched against a VPN-Ipv4 route ("page 8 line 49-51). It is

inferred that the packets contains the information of the device or node from which it came from.

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to have a virtual networking administration in a data-over-cable-system 10 9 column 28 line 18-19) as taught by Fijolek et al. matching a destination address against a VPN-Ipv4 route as taught by Rosen to provide a mechanism that will transmit packets to a specific VPN.

Fijolek et al. does not discloses having the *means for if it is determined that said first node is a member of at least one VPN, binding an ID of said node with said VPN to thereby cause said first node to be associated with said VPN, wherein the ID is bound with the node by an entity other than the node.* Rosen et al. discloses having a method in which a service provider with an IP backbone may provide VPNs (Virtual Private Networks) for its customers with MPLS (Multiprotocol Label Switching) is used for forwarding packets over the backbone (Abstract). It is inferred that this mechanism can be implemented in the head end of a cable system 26. further discloses having a labeled packets ("binding an ID") being associated with specific VPNs (page 16 line paragraph 8.1 line 1-12). It is inferred that the labels indicate which VPN the packet via device or node is destined for.

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to have a virtual network administration in a data-over-cable system Fijolek et al. with a mechanism that will label packet with corresponding

VPNs as taught by Rosen et al. to provide a mechanism that will transmit packets via device or node to there appropriate VPN.

With regard to claim 6, in combination Fijoleck et al. and Rosen et al. teaches the apparatus recited in claim 5. *further including means for mapping a particular sub-interface of the Head End to said particular VPN.* Fijoleck et al. discloses having a head end of cable system in fig. 1. Fijoleck et al. further discloses having a virtual networking administration in a data-over-cable-system 10 using a network address and the first virtual networking tag stored in a virtual networking table associated with the second network device to provide selected first network devices a desired networking service on a virtual network via the data-over-cable-system (column 28 line 34-43). However, Fijoleck et al. does not disclose means for mapping a particular sub-interface of the Head End to said particular VPN. Rosen et al. discloses having a method in which a service provider with a IP backbone may provide VPNs (Virtual Private Networks) for its customers with MPLS (Multiprotocol Label Switching) is used for forwarding packets over the backbone (Abstract). Rosen et al. discloses that one could divide the interface into multiple "sub-interfaces"... and assign the packets to a VPN based on the on the sub-interface over which it arrives (page 7 paragraph 3.1 line 11-17).It is inferred that this mechanism can be implemented in the head end of the data-over-cable-system and that the head end also can limited to a particular VPN.

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to have a virtual networking administration in a data-

over-cable-system 10 as taught by Fijolek et al. assign the packets to a VPN based on the on the sub-interface over which it arrives as taught by Rosen et al. to provide a mechanism that will restrict packets access into VPNs that are not assigned to the packet.

With regard to claim 8, in combination Fijoleck et al. and Rosen et al. teaches the apparatus recited in claim 7. F*urther comprising: means for if it is determined that said first node is a member of a first VPN, determining at said Head End device whether the destination address of said packet is within said first VPN.* Fijoleck et al. discloses having a head end of a cable system 26 with a cable modem termination system 12 in fig. 1. Fijoleck et al. further discloses having a virtual networking administration in a data-over-cable-system 10 (column 28 line 18-19). However, Fijoleck et al. does not discloses that the first node is a member of a first VPN, determining at said Head End device whether the destination address of said packet is within said first VPN. Rosen et al. discloses having a method in which a service provider with an IP backbone may provide VPNs (Virtual Private Networks) for its customers with MPLS (Multiprotocol Label Switching) is used for forwarding packets over the backbone (Abstract). It is inferred that this mechanism can be implemented in the head end of a cable system 26. Rosen et al. further discloses when a packets destination address is matched against a VPN-IPv4 route (page 8 line 49-51).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to have a virtual networking administration in a data-over-cable-system 10 as taught by Fijolek et al. matching packets destination address against a VPN-IPv4 route (VPN) as taught by Rosen et al. to provide a mechanism that will restrict packets from entering in VPNs that they are not associated with.

With regard to claim 9, in combination Fijoleck et al. and Rosen et al. teaches the apparatus recited in claim 7.*further comprising means for routing the packet to the second node.* Fijoleck et at. discloses having a having a head end of a cable system 26 with a cable modem termination system 12 in fig. 1 routing packets to a cable modem... the system configurations may be "one-to-one", "one-to-many" or "many –to-many" (column 7 line 20-38 and fig.1). It is inferred that the head end have the capability to route packets to other cable modems in the network.

6. Claims 10 and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fijoleck et al. (US Patent 6,577,642) in view of Fijolek et al. (US Patent 6,510,162) and Rosen ("BGP/MPLS VPNs", 1999).

With regard to claim 10, Fijoleck et al. discloses having a app*aratus for configuring a Head End of an access network to route packets from a first node to a second node in the access network,* Fijolek et al. discloses having a cable modem termination system 12 in fig 1 located in a head end of cable system 26 (fig.1).

the apparatus comprising: means for associating particular network nodes on the access network with at least one corresponding virtual private network; Fijoleck et al. further discloses having a virtual networking administration in a data-over-cable-system 10 (column 28 line 18-19).

Fijoleck et al. (6,577,642) does not explicitly discloses having the *means for assigning to the first node an ID specific to the access network, wherein the ID is assigned to the first node by an entity other than the first node;* Fijolek et al. (6,510,162) discloses having a cable modem termination system 12 in fig. 1 that assigns service identifiers (SIDs) to CM ("first node", cable modems, column 15 line 17-18).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to have a head end of a cable system 26 with a cable modem termination system 12 Fijolek et al. (6,577,642) assigning service identifiers (SIDs) to CM as taught by Fijolek et al.(6,510,162) to provide a mechanism that will distinguish cable modems within a data-over-cable system.

Fijoleck et al. (6,577,642) does not discloses having the *means for associating the assigned ID with the first VPN to thereby cause the first node to be associated with the first VPN.* Rosen et al. discloses having a method in which a service provider with a IP backbone may provide VPNs (Virtual Private Networks) for its customers with MPLS (Multiprotocol Label Switching) is used for forwarding packets over the backbone (Abstract). Rosen et al. further discloses having a labeled packets ("assigned ID") being

associated with specific VPNs (page 16 line paragraph 8.1 line 1-12). It is inferred that the labels indicate which VPN the packet via device or node is destined for.

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to have a head end of a cable system 26 with a cable modem termination system 12 Fijolek et al. (6,577,642) with a mechanism that will label packet with corresponding VPNs as taught by Rosen et al. to provide a mechanism that will transmit packets via device or node to there appropriate VPN.

With regard to claim 11, in combination Fijoleck et al. and Rosen et al. teaches the apparatus recited in claim 10.*further means for including mapping a particular sub-interface of the Head End to the first VPN.* Fijoleck et al. discloses having a head end of a cable system 26 in fig. 1. Fijolek et al. further disclose having a virtual network administration in a data-over-cable-system (column 28 line 18-19). However, Fijoleck et al. does not disclose means for including mapping a particular sub-interface of the Head End to the first VPN. Rosen et al. discloses that one could divide the interface into multiple "sub-interfaces"... and assign the packets to a VPN based on the on the sub-interface over which it arrives (page 7 paragraph 3.1 line 11-17).It is inferred that this mechanism can be implemented in the head end of the data-over-cable-system and that the head end also can limited to a particular VPN.

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to have a virtual networking administration in a data-

over-cable-system 10 as taught by Fijolek et al. assign the packets to a VPN based on the on the sub-interface over which it arrives as taught by Rosen et al. to provide a mechanism that will restrict packets access into VPNs that are not assigned to the packet .

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to DeWanda Samuel whose telephone number is (571) 270-1213. The examiner can normally be reached on Monday- Thursday 8:30-5:30 EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ricky Q. Ngo can be reached on (571) 272-3139. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

DeWanda Samuel
6/24/2007

RICKY Q. NGO
SUPERVISORY PATENT EXAMINER